日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　９月２９日

出願番号
Application Number: 特願２０００－２９９３０５

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is ＪＰ２０００－２９９３０５

出願人
Applicant(s): 高　振宇

CERTIFIED COPY OF PRIORITY DOCUMENT

２００５年１１月３０日

特許庁長官
Commissioner,
Japan Patent Office

中嶋誠

【書類名】　特許願
【整理番号】　K000-04
【提出日】　平成12年 9月29日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/21
【発明者】
　【住所又は居所】　埼玉県川口市金山町１番４－２０５号シャトープリンス
　【氏名】　高　振宇
【特許出願人】
　【識別番号】　593221598
　【氏名又は名称】　高　振宇
　【国籍】　中華人民共和国
【代理人】
　【識別番号】　100093517
　【弁理士】
　【氏名又は名称】　豊田　正雄
【手数料の表示】
　【予納台帳番号】　030524
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ホームページ改竄防止システム

【特許請求の範囲】

【請求項１】

（１）コンテンツファイルを暗号化処理した暗号化コンテンツファイルを保管する暗号化インターネットウェブサーバー、

（２）前記暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、

（３）ユーザーからアクセス要求を受けた前記暗号化されたコンテンツファイルを復号化してユーザーに送信する手段、

（４）前記暗号化されたコンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルを暗号化処理して作成した暗号化コンテンツファイルにより、前記暗号化インターネットウェブサーバーを更新・復旧処理する手段、

を含むことを特徴とするホームページ改竄防止システム。

【請求項２】

（１）コンテンツファイルに全般の認証を行う認証子を含むデータをヘッダーとして付加した改竄防止ヘッダー付きコンテンツファイルを保管する改竄防止機能付きインターネットウェブサーバー、

（２）前記改竄防止機能付きインターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、

（３）ユーザーからアクセス要求を受けた前記改竄防止ヘッダー付きコンテンツファイルから該ヘッダーを除去したコンテンツファイルをユーザーに送信する手段、

（４）前記改竄防止ヘッダー付きコンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルに改竄防止ヘッダーを附加して作成した改竄防止ヘッダー付きコンテンツファ

イルにより、前記改竄防止機能付きインターネットウェブサーバーを更新・復旧処理する手段、
を含むことを特徴とするホームページ改竄防止システム。

【請求項３】

（１）コンテンツファイルを暗号化処理した暗号化コンテンツファイルに全般の認証を行う認証子を含むデータをヘッダーとして付加した改竄防止ヘッダー付き暗号化コンテンツファイルを保管する改竄防止機能付き暗号化インターネットウェブサーバー、

（２）前記改竄防止機能付き暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、

（３）ユーザーからアクセス要求を受けた前記改竄防止ヘッダー付き暗号化コンテンツファイルから該ヘッダーを除去し、復号化してユーザーに送信する手段、

（４）前記改竄防止機能付き暗号化コンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルを暗号化処理し、改竄防止ヘッダーを附加して作成した改竄防止ヘッダー付き暗号化コンテンツファイルにより、前記改竄防止機能付き暗号化インターネットウェブサーバーを更新・復旧処理する手段、
を含むことを特徴とするホームページ改竄防止システム。

【請求項４】

（１）コンテンツファイルに全般の認証を行う認証子を含むデータをヘッダーとして付加した改竄防止ヘッダー付きコンテンツファイルを暗号処理した改竄防止機能付き暗号化コンテンツファイルを保管する改竄防止機能付き暗号化インターネットウェブサーバー、

（２）前記改竄防止機能付き暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、

（３）ユーザーからアクセス要求を受けた前記改竄防止ヘッダー付き暗号化コンテンツファイルを復号化し、改竄防止ヘッダーを除去してユーザーに送信する手

段、

（４）前記改竄防止機能付き暗号化コンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルに改竄防止ヘッダーを附加し、暗号化処理して作成した改竄防止ヘッダー付き暗号化コンテンツファイルにより、前記改竄防止機能付き暗号化インターネットウェブサーバーを更新・復旧処理する手段、

を含むことを特徴とするホームページ改竄防止システム。

【請求項５】

前記暗号化および復号化処理がカオス暗号法により行われることを特徴とする請求項１乃至４記載のホームページ改竄防止システム。

【請求項６】

前記認証がカオス理論を用いたメッセージ認証技術を用いた方法により行われることを特徴とする請求項２至４記載のホームページ改竄防止システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネットにおけるサーバーシステムに関する。さらに詳細には、ホームページ改竄防止システムに関する。

【０００２】

【従来の技術】

インターネットは、基本ルール（ＴＣＰ／ＩＰプロトコル）に乗っ取っていれば、ネットワーク上の任意の場所にアプリケーション環境を構築できる。このシステムの柔軟性がインターネットの利点であるが、逆にそれがハッカー（システム不法侵入者）の標的になりやすいというセキュリティ上の弱点がある。現に官庁のホームページが何者かに書き換えられ、社会問題となったことも記憶に新しい。

【０００３】

従来のウェブサーバーには、html、画像、音声などのコンテンツファイルはそのまま保存され、ブラウザからの請求が来たら、関連するファイルを出すという

ような基本仕組みである。従って、ハッカーなどは何らかの方法でウェブサーバーに侵入すれば、簡単にhtmlなどファイルを改竄できる。特に、ホームページシステムは、ラジオ・テレビと同じように多くの人に見てもらうために、ファイヤウォール外に置き、非常に攻撃されやすい。さらに、TELNET・FTPのようなアプリと異なって、リクエストに対して直接回答をしてセッションを切断するというようなアーキテクチャであるので、身元認証と追跡が非常に困難である。

【０００４】

このような攻撃に対するものとして、ホームページ監視システムのような技術がある。基本原理は、以下のようなものである。ウェブサーバーに置くコンテンツファイルに対して、図１に示すように常時ホームページをチェック（監視）している。すなわち、図において、

Ｐ１→Ｐ２→Ｐ３→……→Ｐｉ→……→Ｐｓ→……→Ｐｎ→Ｐ１→Ｐ２→…の順にサイクリックにページデータをチェックしている。改竄が認められた時点で、そのコンテンツファイルの公開中止あるいは元データで置き換えるなどの対策が要求されるところである。

【０００５】

この方法の問題点として、①システムの規模（コンテンツファイル数）及びコンピュータのパワー性能にもよるが、現実のシステムでは、全部ファイルを一回にチェックするため、普通、数分間から数十分間かかる。この間に、改竄されたファイルが、ユーザからのアクセス要求があったら、改竄されたまま状態で送り出してしまう。即ち、１００％の改竄防止できない。②監視サーバーは２４時間でフール稼動しなければならないので、システムに非常に負荷が掛かってしまい、ウェブサーバーのレスポンスが低下、CPUのパワーが足りなくなるという結果が避けられない。その結果、大型システムに向かない。

【０００６】

【発明が解決しようとする課題】

従来技術で述べたように、ファイアウォール内にホームページを設けることは、必ずも容易な技術でないし、仮に可能だとしても（実際に可能だが）、経済的問題、不特定多数を相手にしたときの処理速度とオープン性の維持の問題、内部

ネットワークへの悪影響などの、様々な問題がある。ファイアウォールと一言で言っても、どれだけセキュリティを高めるかによって、リアルタイム侵入検知の仕方が異なり、かりに検知基準を厳しくすれば一般のユーザー（クライアント）がホームページをアクセスできなくなる恐れがあり、オープン性が失われてしまうことになる。

【０００７】

一方、裸の状態（直接インターネットに接続状態）でウェブサーバーを設置した場合には、図１の例に挙げたような改竄検知の方法もあるが、この方法にも以下のような問題がある。すなわち、ページデータが増えた場合、全ページを１回チェックするだけ１０分とか２０分も掛かってしまうことである。たとえば、図１の例で１サイクルのチェック時間が１０分とした場合、ＰｓのデータをチェックしているときにP_i（$i<s$）のデータが改竄されたとすると、ＰｓからP_iに次のチェックが回ってくるまでの数分間は、改竄データがそのままインターネットユーザーに開放された状態になっていることである。

【０００８】

本発明が対象にしている課題は、ホームページの改竄にどのように対処するかである。なぜなら、改竄はときには取り返しのつかない社会的な問題を起こすこともある。“サイバーモールにおける商品カタログ用ホームページの商品価格が“１０万円”が“１００円”に書き換えられていたとすれば、業者と消費者の間のトラブルの原因ともなりかねない。

【０００９】

本発明が解決しようとする課題は、(1)改竄した行為があったとしても、改竄されたコンテンツファイルを外（アクセス者）へ送り出さないこと。(2)ハッカーがウェブサーバーに侵入したとして、意味がある改竄が出来ないこと。(3)ホームページを提供しているウェブサイトに対して、従来の形態をできるだけ踏襲し、経済的にも、また技術的にも、容易に導入できるホームページ改竄防止システムを開発することである。

【００１０】

【課題を解決するための手段】

上記の課題を解決するために、請求項１に記載された本発明は、（１）コンテンツファイルを暗号化処理した暗号化コンテンツファイルを保管する暗号化インターネットウェブサーバー、（２）前記暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、（３）ユーザーからアクセス要求を受けた前記暗号化されたコンテンツファイルを復号化してユーザーに送信する手段、（４）前記暗号化されたコンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルを暗号化処理して作成した暗号化コンテンツファイルにより、前記暗号化インターネットウェブサーバーを更新・復旧処理する手段、を含むことを特徴とするホームページ改竄防止システムである。

【００１１】

請求項２に記載された発明は、（１）コンテンツファイルに全般の認証を行う認証子を含むデータをヘッダーとして付加した改竄防止ヘッダー付きコンテンツファイルを保管する改竄防止機能付きインターネットウェブサーバー、（２）前記改竄防止機能付きインターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、（３）ユーザーからアクセス要求を受けた前記改竄防止ヘッダー付きコンテンツファイルから該ヘッダーを除去したコンテンツファイルをユーザーに送信する手段、（４）前記改竄防止ヘッダー付きコンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルに改竄防止ヘッダーを附加して作成した改竄防止ヘッダー付きコンテンツファイルにより、前記改竄防止機能付きインターネットウェブサーバーを更新・復旧処理する手段、を含むことを特徴とするホームページ改竄防止システムである。

【００１２】

請求項３に記載された発明は、（１）コンテンツファイルを暗号化処理した暗号化コンテンツファイルに全般の認証を行う認証子を含むデータをヘッダーとして付加した改竄防止ヘッダー付き暗号化コンテンツファイルを保管する改竄防止

機能付き暗号化インターネットウェブサーバー、（２）前記改竄防止機能付き暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、（３）ユーザーからアクセス要求を受けた前記改竄防止ヘッダー付き暗号化コンテンツファイルから該ヘッダーを除去し、復号化してユーザーに送信する手段、（４）前記改竄防止機能付き暗号化コンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルを暗号化処理し、改竄防止ヘッダーを附加して作成した改竄防止ヘッダー付き暗号化コンテンツファイルにより、前記改竄防止機能付き暗号化インターネットウェブサーバーを更新・復旧処理する手段、を含むことを特徴とするホームページ改竄防止システムである。

【００１３】

請求項４に記載された発明は、（１）コンテンツファイルに全般の認証を行う認証子を含むデータをヘッダーとして付加した改竄防止ヘッダー付きコンテンツファイルを暗号処理した改竄防止機能付き暗号化コンテンツファイルを保管する改竄防止機能付き暗号化インターネットウェブサーバー、（２）前記改竄防止機能付き暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウオール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、（３）ユーザーからアクセス要求を受けた前記改竄防止ヘッダー付き暗号化コンテンツファイルを復号化し、改竄防止ヘッダーを除去してユーザーに送信する手段、（４）前記改竄防止機能付き暗号化コンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルに改竄防止ヘッダーを附加し、暗号化処理して作成した改竄防止ヘッダー付き暗号化コンテンツファイルにより、前記改竄防止機能付き暗号化インターネットウェブサーバーを更新・復旧処理する手段、を含むことを特徴とするホームページ改竄防止システムである。

【００１４】

請求項５に記載された発明は、前記暗号化および復号化処理がカオス暗号法により行われることを特徴とする請求項１乃至４記載のホームページ改竄防止シス

テムである。請求項６に記載された発明は、前記認証がカオス理論を用いたメッセージ認証技術を用いた方法により行われることを特徴とする請求項２至４記載のホームページ改竄防止システムである。

【００１５】

本発明のシステムをさらに具体的に説明すると、以下のようになる。html、画像、音声などのコンテンツファイルを保管する通常のウェブサーバー、および前記コンテンツファイルに全般に認証を行う認証子を含むデータをヘッダーとして付加したヘッダー付きコンテンツファイルを保管する改竄防止機能付きウェブサーバーを備えたホームページ改竄防止システムにおいて、(1)前記ヘッダーを附加したコンテンツファイルに対して、ユーザーからアクセス要求を受けた時点で、改竄があったかどうかの認証チェックを行う手段、(2)前記認証チェックが改竄なしであれば前記ヘッダーを除去したコンテンツファイルをユーザーに送信する手段、(3)前記認証チェックが改竄ありであれば、前記ユーザーにコンテンツファイルを送信せず、前記ファイアウォール等で隔離されたコンテンツファイルを保管するサーバーから前記インターネットウェブサーバーへ、改竄されたコンテンツファイルに対応するコンテンツファイルに認証子を含むデータをヘッダーとして附加したヘッダー付きコンテンツファイルで、改竄されたコンテンツファイルを更新して復旧する手段、を備えたシステムとする。

【００１６】

html、画像、音声などのコンテンツファイルを保管する通常のウェブサーバー、および前記コンテンツファイルを暗号化し、全体に認証を行う認証子を含むデータをヘッダーとして付加したヘッダー付き暗号化コンテンツファイルを保管する改竄防止機能付きウェブサーバーを備えたホームページ改竄防止システムにおいて、(1)前記ヘッダー付き暗号化コンテンツファイルに対して、ユーザーからアクセス要求を受けた時点で、改竄があったかどうかの認証チェックを行う手段、(2)前記認証チェックが改竄なしであれば前記ヘッダーを除去した暗号化コンテンツファイルを復号化してユーザーに送信する手段、(3)前記認証チェックが改竄ありであれば、前記ユーザーにコンテンツファイルを送信せず、前記ファイアウォール等で隔離されたコンテンツファイルを保管するサーバーから前記イン

ターネットウェブサーバーへ、改竄されたコンテンツファイルに対応するコンテンツファイルを暗号化し、全体に認証を行う認証子を含むデータをヘッダーとして附加したヘッダー付き暗号化コンテンツファイルで、改竄されたコンテンツファイルを更新して復旧する手段、を備えたシステムである。

【００１７】

また、暗号法がカオス理論を用いた暗号法であり、前記認証がカオス理論を用いたメッセージ認証技術を用いた場合は特に優れたホームページ改竄防止システムとなる。

【００１８】

図２は本発明のシステムの全体的な概念を示す図である。本発明では、コンテンツ全体に対する認証を行う。認証チェックで改竄を検知したとき、ページ全体を送信せず、また、認証チェックで改竄を検知した場合には、システム管理者に知らせる手段を備えておけば、改竄に対する対処が速やかに行える。当然、ログ（履歴）も記録することが好ましい。

【００１９】

コンテンツの暗号化を行う請求項２記載の発明では、改竄データを意味のあるデータとして（書き換えた内容のままで）インターネットユーザー（ソフトウェアで表現すればブラウザ）に送信しない。本発明ではコンテンツファイルを暗号化して保持し、ページアクセス要求を受けた時点で復号化し、ユーザーに送信する。この方法を用いれば、システム侵入者がページデータを書き換えたとしても、その内容が直接ユーザーに送信されることはない。なぜなら、ページデータは復号化してユーザーに送信されるので、復号化により意味不明の内容に変化するからである。侵入者が暗号化された形でページデータを書き換えない限り、その書き換えたデータが意味ある内容として送信されることはない。

【００２０】

インターネットユーザーに開放するのは改竄防止機能付きウェブサーバーのコンテンツファイルであり、通常のウェブサーバーのコンテンツファイルは維持管理用およびバックアップ用として保管管理する。すなわち、ホームページの更新や追加などがある場合には、まず通常のコンテンツファイルに対して更新・追加

処理をし、動作確認を行う。その後、暗号化して改竄防止機能付きコンテンツファイルに移す。通常のサーバー内のコンテンツファイルを直接インターネットユーザーに開放することはない。

【００２１】

先に、改竄が「あり」と判断された場合には、改竄データを含むコンテンツファイルに対して、通常のサーバーと改竄防止機能付きウェブサーバーの形態をとっているので、改竄データを元のデータで差し替える方法が可能である。即ち、自動的に復旧することができる。

【００２２】

すなわち、通常のサーバーで元の平文Ｍに対して、ChaosMAMのような認証技術を用いて平文Ｍのメッセージ認証子ＭＡＣを作成しておき、改竄防止機能付きウェブサーバーで作成するメッセージ認証子ＭＡＣ’をＭＡＣと照合して異なる場合には「改竄あり」と判断し、改竄防止機能付きサーバーから通常のサーバーにＭを要求して、改竄されたＭ’をＭで置き換える。

【００２３】

【発明の実施の形態】

図３は、本発明の暗号を用いるホームページ改竄防止システムの基本システム構成図である。元データとなるコンテンツファイル（以降、“元データコンテンツファイル”と記述）はホームページ管理コンピュータで作成する。一般的にコンテンツファイルは有機的なページのつながりをもって構成されているから、通常データベース化されている。ただし、本稿においては単に“ファイル”または“ＨＴＭＬファイル”と記述するが、その構造上の形式までは問わない。いずれにしろ、ホームページ管理コンピュータで作成した元データコンテンツファイルは通常の形式のコンテンツファイルである。この元データコンテンツファイルをウェブサーバーに移すときに暗号化し、認証子を含むヘッダーを付けて、暗号化されたコンテンツファイル（以降、“暗号化コンテンツファイル”と記述）を作成する。

【００２４】

元データコンテンツファイルはインターネットと切り離した状態で保存する必

要がある。ユーザー（ブラウザ）からページ要求（アクセス）があると、ウェブサーバーは該当する暗号化コンテンツファイルを抽出し、認証チェック後に、ヘッダー部を切り離して、復号化してユーザーに送信する。

【００２５】

本発明はホームページ改竄防止システムであるが、コンテンツファイルを暗号化する方式では、改竄があったとしても、その改竄が意味のないものとすることができる。図４の例で説明しよう。（１）はウェブサーバー上のページデータ（ＨＴＭＬファイル）、（２）は改竄された内容（下線部が改竄個所、“はる”→“あき”）、（３）はユーザーに送信される内容である。従来技術では、改竄された内容がそのまま送信されてしまう。一方、コンテンツファイルを暗号化する本発明の方式下では、サーバー上では暗号化コンテンツファイルになっていて、しかもブラウザからのアクセスに対しては復号化してユーザーに送信するために、改竄データがそのままユーザーに届くことはない。なお図５の暗号化は、アイウエオ五十音表で隣り合う文字を後ろに１文字ずらしただけである。

【００２６】

暗号化と復号化の組み合わせでは、図４の例のように意味の分からないコンテンツがホームページ画面に表示される。改竄者の意図をくじくという面では成功しているが、少なくても、ホームページ提供者としても好ましいことではない。また、改竄データが復号化されたとき、偶然別の意味のある内容にならないとも限らない。

【００２７】

さらに、不法侵入者が暗号文（暗号化コンテンツファイルのページデータ、図４の（１））とホームページ上のデータ（図４の（３））を見比べることによって、暗号コードと平文の単語の対応がつけば、単語レベルの暗号による書き換えがされる危険性は残っている。

【００２８】

本発明ではメッセージ認証を行っているのでこのような事態は生じない。図５に示すように、メッセージ認証は、送信側で送信メッセージと暗号鍵（秘密鍵）からメッセージ認証子ＭＡＣ（Message Authentication Code）を作成し、メッ

セージとＭＡＣを送信する。受信側は受信したメッセージM’（改竄されている可能性があるからＭとは限らない）と、保持している鍵（秘密鍵あるいは公開鍵）とからメッセージ認証子ＭＡＣ’を作成し、ＭＡＣとＭＡＣ’をチェックし、等しければメッセージの正当性が証明され、等しくなければメッセージに何らかの改竄があったと判断できる。

【００２９】

本発明では、カオス暗号法、及びカオス理論によるカオス認証技術（ChaosMAM）は、速度とセキュリティ強度の面で最も適当であるが、他の暗号方法でも可能である。よく知られた暗号法としては共通鍵暗号方式のＤＥＳ（Data Encryption Standard）がある。図６は、ＤＥＳを用いたメッセージ認証子の作成例である。ＤＥＳでは平文Ｍ（暗号前のメッセージ）を６４ビットのブロックに分割し、各ブロックＭｉに対して

Ｃｉ＝ＤＥＳ（Ｋ，Ｃｉ－１．ＸＯＲ．Ｍｉ）

を作成する。

【００３０】

ここで、ＤＥＳ（…）はＤＥＳのアルゴリズムを表し、ＸＯＲ．は排他的論理和（図では丸印の中に＋を記述した記号）を表す。また、Ｋは秘密鍵であり、送信側と受信側で共通して保持している鍵である。認証文Ｃｉは１つ前の認証文Ｃｉ－１とブロック化メッセージＭｉとの排他的論理和で作られる文に対して、鍵Ｋで暗号化したメッセージである。

すなわち、認証文Ｃ１を除いて、認証文Ｃｉは純粋にブロック化平文Ｍｉを暗号化したものではない。

【００３１】

したがって、メッセージ認証子ＭＡＣから元のメッセージ（平文ＭまたはＭｉ）を導くことはできない。認証子の目的は暗号化ではなく、送信したメッセージ（平文）の正当性をチェックするものであるからである。この例では、認証子ＭＡＣは最後の認証文Ｃｎの上位３２ビットを抽出してものである。なお、ここの認証子作成例は、認証文ＣｉはＣｉ＋１と連動していることから、「ＤＥＳのＣＢＣ（Cipher Block Chaining）モードによる認証子法」とよばれる。

【００３２】

平文M’または暗号文C’（送信側の発信時はMまたはC）を受信した受信側では、平文M’と暗号文C’（C’受信時は平文M’に復号化、M’で受信時は暗号文C’に暗号化）から認証子ＭＡＣ’を導き、同時に送られてきたＭＡＣと比較して、送信途中に改竄があったかどうかを判定する。

【００３３】

図９に、本発明の暗号化ファイルの構造を示す。附加されたヘッダー情報には、認証子ＭＡＣ、サイズなどの情報が書き込まれる。本発明のシステムでは、カオス暗号法、およびカオス理論によるカオス認証技術は、速度の面で最も適当であるが、他の暗号方法でも原理的には可能である。

【００３４】

本発明においては、図７に示すように通常のウェブサーバーで暗号化と認証子作成を行い、改竄防止機能付きウェブサーバーに送信する。ウェブサーバーではページデータをユーザーに送信する時点で、暗号文Ｃ（暗号化されたページデータ）を復号化して平文Ｍ（元のページデータ）に変換するとともに、認証子ＭＡＣで平文Ｍの認証を行う。ホームページ管理コンピュータで作成した認証子ＭＡＣとウェブサーバーで作成した認証子ＭＡＣ’が一致しないときには、暗号文Ｃに何らかの改竄があったと判定する。改竄があった場合、そのコンテンツファイルを送信しない。まだ、同時に復旧と警報を行う。

【００３５】

なお、認証子ＭＡＣｉで行う方法を実施例で説明する。また、改竄されたコンテンツファイルデータをリアルタイムに修復してユーザーに送信する方法も実施例で説明する。

【００３６】

【実施例】

本発明の実施例をGCCカオス暗号法とChaosMAMカオス認証技術を用いた場合の例で説明する。まず、簡単にカオス暗号法を説明する。カオス暗号法では公開鍵暗号方式と共通鍵暗号方式が使えるが、ここでは共通鍵暗号方式で説明する。本発明の場合も、ユーザーに鍵を渡す必要がないために、共通鍵暗号方式で十分で

きる。いま平文M、カオス関数G、暗号文C、暗号鍵Kとしたとき、

　　C＝G（K，M）

と暗号化できる。暗号文Cを復号化するには、カオス逆関数G－1と鍵Kを用いて、

　　M＝G－1（K，C）

と復号化できる。カオス暗号法においては平文Mの長さは自由である。鍵Kの長さは可変長で、８から２０４８ビットである。

【００３７】

本発明は、①Chaos Web Serverと②エンコーダー/デコーダーモジュールと③復旧Server/Clientと④警報システムなど部分から構成。そこで、①Chaos Web Serverでは通常のウェブサーバーの全部機能＋デコーダー機能、まだ、②エンコーダー/デコーダーモジュールでは暗号化、認証子付け、ヘッダー情報を付けるなど機能を実行するエンコーダー部分及び、認証チェック、復号化、ヘッダー情報を切れるなど機能を実行するデコーダー部分、③復旧Serverの中にエンコーダーの機能が入っている。

【００３８】

図８は、本発明のコンテンツファイルを暗号化するホームページ改竄防止システムを概念的に示したシステム構成図である。基本的に図２に示したシステム構成と同じであるが、改竄防止機能付きウェブサーバーのコンテンツファイルが暗号化されていることと、クライアントを介して暗号化コンテンツファイルの更新を行っていること、および暗号化にカオス暗号法が用いられていることである。

【００３９】

ホームページのＨＴＭＬファイルを含むコンテンツファイルをホームページ管理用サーバー上に持ち、復旧サーバーを通じて、コンテンツファイルをＧＣＣ暗号化とＭＡＭ認証子＜ＭＡＭ　ＭＡＣ：Message Authentication Methodによる認証子の意味＞）生成、及びファイルサイズ、日付、認証子などを含むヘッダー情報部分を追加するというエンコーダーを行い、ファイアウォールの外側に設置した復旧サーバーの管理下にある復旧クライアントに送信する。復旧クライアントは、受信したエンコーダーされたコンテンツファイルを復旧サーバーの指示し

た場所に置く。ネットワークユーザーからページ要求があった場合、改竄防止機能付きウェブサーバーは、(1)エンコーダーされたコンテンツファイルのヘッダー部分から、認証子などの情報を読み出し、(2)認証チェックを行い、認証にパスしたときには、ヘッダー部分を切り捨て、復号化を行う、というデコーダー操作をして、元に復帰されたコンテンツファイルをユーザーに送り出す。

【００４０】

もし認証で改竄が認められた場合には、復旧クライアントを通じて、復旧サーバーへ改竄されたファイルを更新する請求を出し、復旧サーバーが請求に応じて、指定ファイルを通常のサーバーから取り出して、エンコーダーして、改竄防止機能付きサーバーへ送り出す、というような復旧を行う。また同時に、警報サーバーにその旨を伝え、警報サーバーから公衆回路を通じてシステム管理者に不法侵入者の存在を知らせる。

【００４１】

【発明の効果】

本発明のシステムによれば、以下のような効果を奏することができる。本発明は、webリアルタイム・チェック技術を実現するものである。高速性の点では、ブラウザからの請求が来た瞬間に、認証チェック、復号を瞬時に行い、チェックシステムがない場合と比べてレスポンス速度は変わらない。安全性の点では、改竄行為があったとしても改竄されたファイルを外（ブラウザ側）に送り出さない。

【００４２】

大型システムに対しても、（１）トラフィックを増加しないのでウェブサーバーに負荷を増加させない。（２）ホームページシステムの規模（ファイル数）が増大しても、チェック時間と復旧速度に影響を与えない。本発明のシステムはブラウザに影響は与えない。従来のブラウザソフトはそのまま使用でき、新しいクライアントソフトをダウンロードする必要はない。本発明のシステムは、ダイナミックな復旧機能を持っている。改竄を発見すると、自動的に高速で元のファイルを入れ替える。また、自動警報機能を設けることもでき、改竄を発見すると、自動的にシステム管理者の携帯電話、ポケベルに発信する。さらに、本発明のシ

ステムは導入しやすく、既存のホームページ編集システムに影響を与えない。本発明のシステムでは、Chaos Web Server１台を導入、ポリシー管理システムを既存のWeb Serverにインストール、簡単なセッティングをすればOK（基本のWeb Server管理知識が必要）である。

【００４３】

本発明のシステムによれば、ホームページ編集者は慣れているツールを用いることができるので、現在のホームページの環境を変えずに、ホームページをデザインしたり、作成したり、更新したりする事が出来る。そして、自動的に最新のホームページのコンテンツファイルを暗号化、認証子　を附加してウェブサーバーに送ることができる。

【００４４】

本発明のシステムでは、(1)改竄行為があったとしても、改竄されたコンテンツファイルを外部（アクセス者）へ送り出すことがないこと、(2)ハッカーがウェブサーバーに侵入したとして、コンテンツファイルが暗号化されている場合は意味がある改竄が出来ないことなどが実現できる。

【００４５】

さらに、本発明の改竄防止システムは、現在のウェブサイト（すでにホームページを開設しているサイト）においてもシステムの全面的な更新を行わなくても容易に導入ができるというメリットがある。しかも、特別な装置や技術を必要としないために経済的負担も少ない。一方、ユーザーが用いるブラウザに対しては何の負担もなく、現在使用しているものがそのまま使える（インターネットへ送り出すときは従来通りのページデータであるため）。すなわちインターネットユーザーへの負担は一切ない。

【００４６】

特に、カオス暗号法とChaosMAM認証技術を用いることによって、以下のような優れた効果が得られる。安全性が高い（新しい暗号法であり、暗号法が解読される可能性がきわめて低い）、処理速度が速く、システムへの負担が少なく、リアルタイムの処理が可能（暗号化、復号化、認証チェック速度が速い）、ブラウザソフトへの影響はゼロ、認証チェックはページ要求が出された時点であるから、

改竄ブロックの自動差し替え処理速度が要求され、その暗号法としてもカオス暗号法は最適である。

【図面の簡単な説明】

【図１】

従来技術における改竄チェック方法を説明する図である。

【図２】

本発明のシステムの概念を説明するためのシステム構成図である。

【図３】

本発明のホームページ改竄防止システムの概念を説明するためのシステム構成図である。

【図４】

本発明の改竄防止の原理を説明するための例である。

【図５】

本発明においてメッセージ認証を説明するための図である（内容自体は従来技術に属する）。

【図６】

本発明においてＤＥＳを用いたメッセージ認証子ＭＡＣを作成する例を示した図である。

【図７】

本発明のウェブサーバーとページ管理コンピュータとの関連を認証子と暗号文との関連で見た説明図である。

【図８】

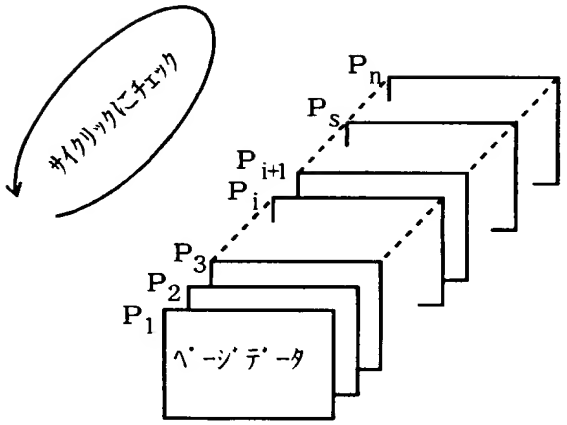
本発明の実施例におけるカオス暗号法を用いたホームページ改竄防止システムのシステム構成図である。

【図９】

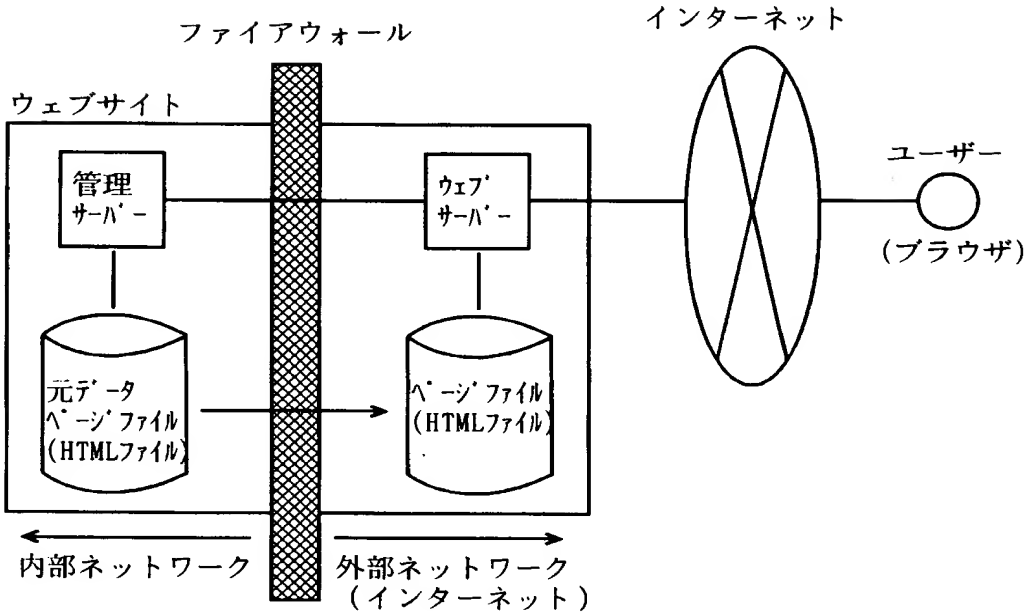
本発明における暗号化ファイルの構造の説明図である。

【書類名】　図面

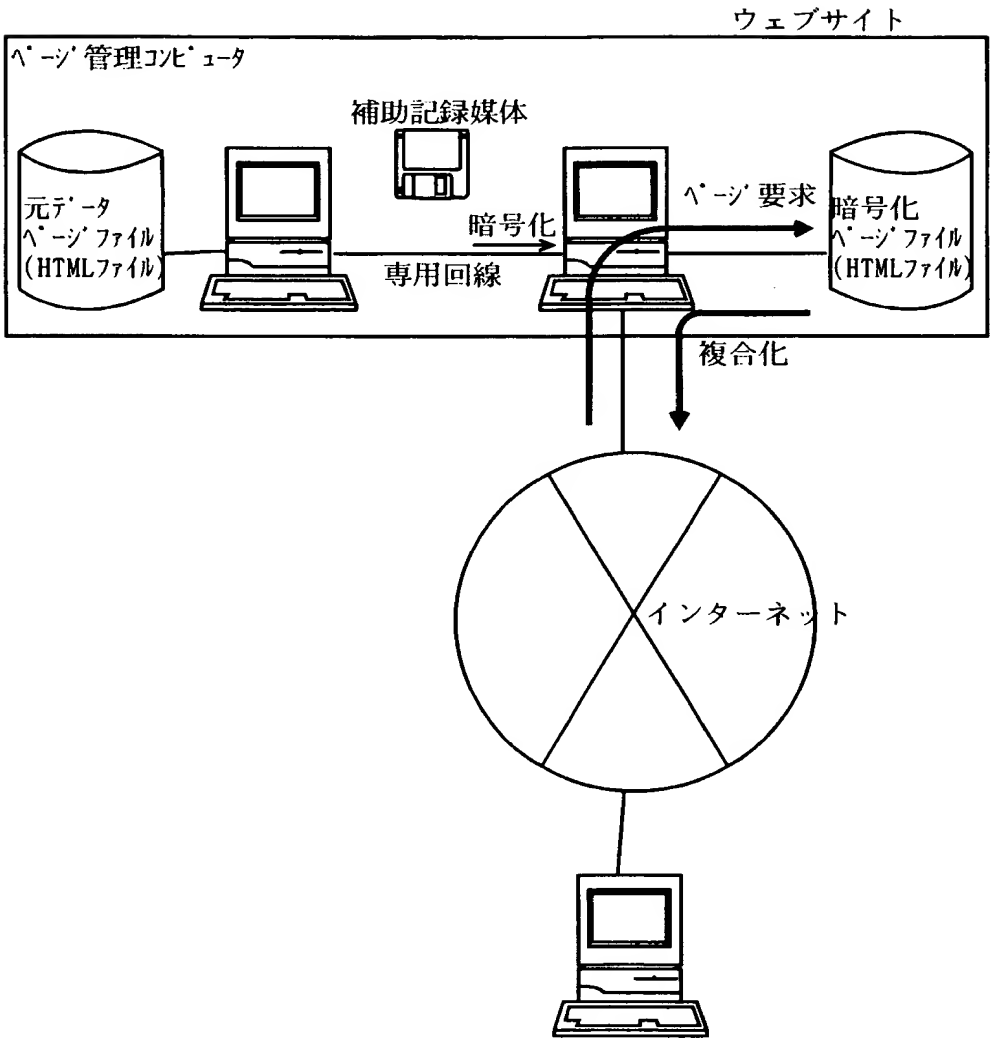
【図１】


サイクリックにチェック
Pn
Ps
Pi+1
Pi
P3
P2
P1
ページデータ

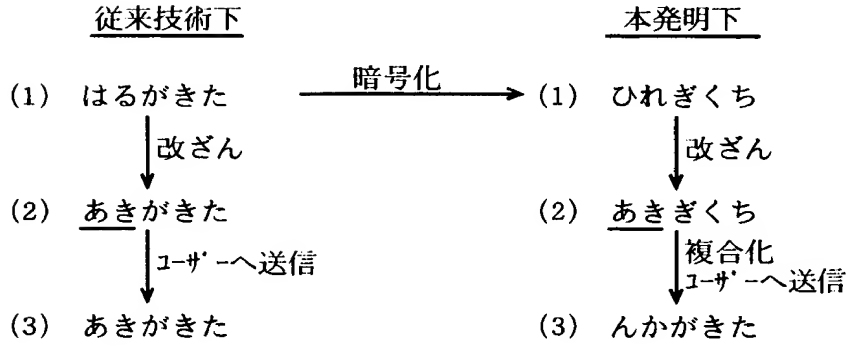
【図２】


ファイアウォール
インターネット
ウェブサイト
管理
サーバー
ウェブ
サーバー
ユーザー
（ブラウザ）
元データ
ページファイル
(HTMLファイル)
ページファイル
(HTMLファイル)
内部ネットワーク
外部ネットワーク
（インターネット）

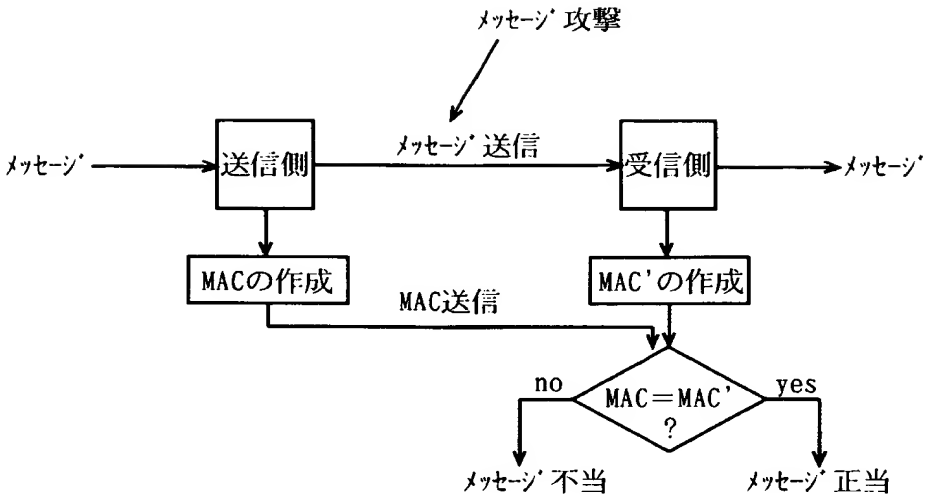
【図３】


ウェブサイト
ﾍﾟｰｼﾞ管理ｺﾝﾋﾟｭｰﾀ
補助記録媒体
元ﾃﾞｰﾀ
ﾍﾟｰｼﾞﾌｧｲﾙ
(HTMLﾌｧｲﾙ)
暗号化
専用回線
ﾍﾟｰｼﾞ要求
暗号化
ﾍﾟｰｼﾞﾌｧｲﾙ
(HTMLﾌｧｲﾙ)
複合化
インターネット

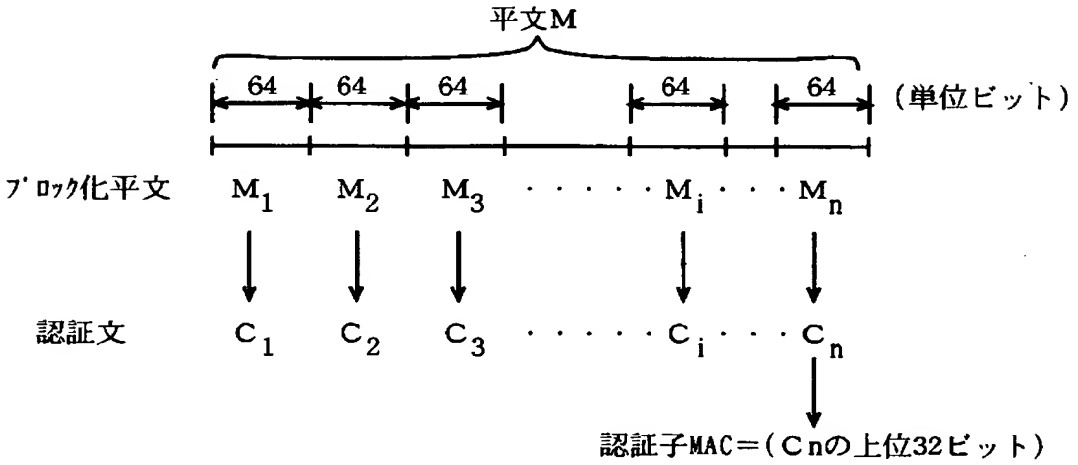
【図４】


従来技術下
本発明下
暗号化
(1) はるがきた
改ざん
(2) あきがきた
ﾕｰｻﾞｰへ送信
(3) あきがきた
(1) ひれぎくち
改ざん
(2) あきぎくち
複合化
ﾕｰｻﾞｰへ送信
(3) んかがきた

【図５】



【図６】



(アルゴリズム)

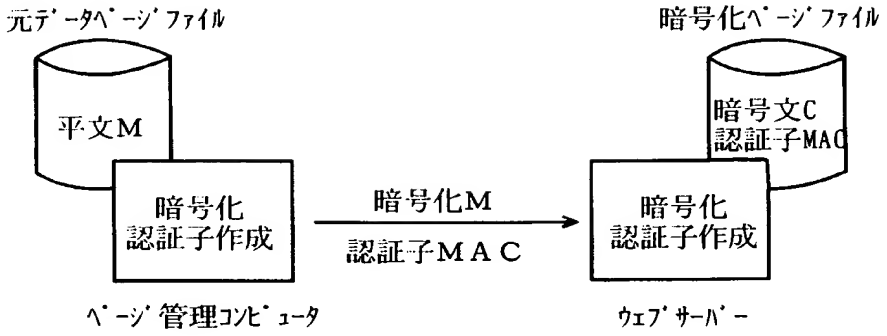
$$C_i = DES(K,\ C_{i-1} \oplus M_i) \qquad (i=2,3,\cdots,n)$$

ただし

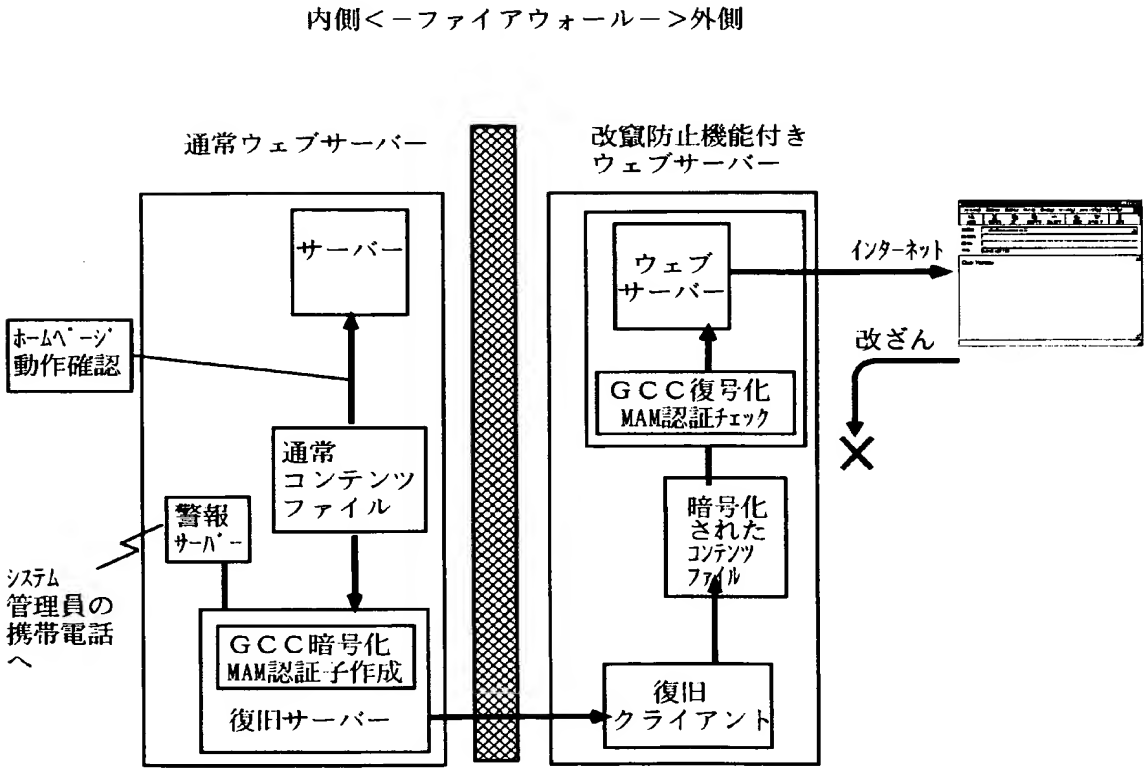
$$C_1 = DES(K,\ M_i)$$

$\oplus$ は排他的論理和(XOR)を表す。

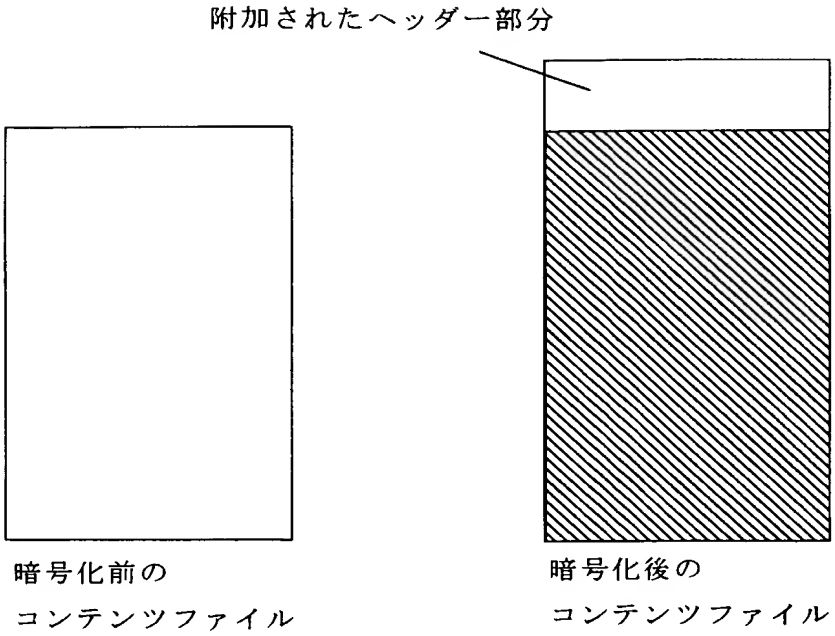
【図７】


元ﾃﾞｰﾀﾍﾟｰｼﾞﾌｧｲﾙ
平文M
暗号化
認証子作成
暗号化M
認証子ＭＡＣ
暗号化ﾍﾟｰｼﾞﾌｧｲﾙ
暗号文C
認証子MAC
暗号化
認証子作成
ﾍﾟｰｼﾞ管理ｺﾝﾋﾟｭｰﾀ
ｳｪﾌﾞｻｰﾊﾞｰ

【図８】


内側<－ファイアウォール－>外側
通常ウェブサーバー
改竄防止機能付き
ウェブサーバー
サーバー
ホームページ
動作確認
通常
コンテンツ
ファイル
警報
サーバー
システム
管理員の
携帯電話
へ
ＧＣＣ暗号化
MAM認証子作成
復旧サーバー
ウェブ
サーバー
ＧＣＣ復号化
MAM認証チェック
暗号化
された
コンテンツ
ファイル
復旧
クライアント
インターネット
改ざん

【図９】



【書類名】　　要約書

【要約】

【課題】　改竄されたコンテンツファイルを外（アクセス者）へ送り出すことがないこと、ハッカーが侵入しても、意味がある改竄が出来ないこと、さらに、ホームページを提供しているウェブサイトに対して、従来の形態をできるだけ踏襲し、経済的にも、また技術的にも、容易に導入できるホームページ改竄防止システムを開発する。

【解決手段】　（１）コンテンツファイルを暗号化処理した暗号化コンテンツファイルを保管する暗号化インターネットウェブサーバー、（２）前記暗号化インターネットウェブサーバーと不正アクセスを排除するファイアウォール等を介して接続し、前記コンテンツファイルを保管するコンテンツファイル保管サーバー、（３）ユーザーからアクセス要求を受けた前記暗号化されたコンテンツファイルを復号化してユーザーに送信する手段、（４）前記暗号化されたコンテンツファイルの改竄を検出したとき、前記コンテンツファイル保管サーバーに保管されている対応するコンテンツファイルを暗号化処理して作成した暗号化コンテンツファイルにより、前記暗号化インターネットウェブサーバーを更新・復旧処理する手段、を含むシステムとする。

【選択図】　　図８

特願２０００－２９９３０５

出　願　人　履　歴　情　報

識別番号　［５９３２２１５９８］

１．変更年月日　１９９５年１２月　６日
［変更理由］　住所変更
住　所　埼玉県川口市西青木１－２３－２８　ロイラルコーポ６０２室
氏　名　高　振宇

２．変更年月日　２０００年１０月１０日
［変更理由］　住所変更
住　所　埼玉県川口市西青木１－２３－２８　ロイラルコーポ６０２室
氏　名　高　振宇